ELLIPTIC CURVES WITH p-SELMER GROWTH FOR ALL p

ALEX BARTEL

Abstract. It is known, that for every elliptic curve over $\mathbb{Q}$ there exists a quadratic extension in which the rank does not go up. For a large class of elliptic curves, the same is known with the rank replaced by the 2-Selmer group. We show, however, that there exists a large supply of semistable elliptic curves $E/\mathbb{Q}$ whose 2-Selmer group goes up in every bi-quadratic extension and for any odd prime p, the p-Selmer group goes up in every D_{2p}-extension and every elementary abelian p-extension of rank at least 2. We provide a simple criterion for an elliptic curve over an arbitrary number field to exhibit this behaviour. We also discuss generalisations to other Galois groups.

1. Introduction

In [6] it is shown that there exist elliptic curves over number fields for which in every qudratic extension of the base field either the rank goes up or the Tate-Shafarevich group becomes infinite. Equivalently, every quadratic twist of such a curve has either positive rank or an infinite Tate-Shafarevich group (the latter is of course conjectured to never happen). Over $\mathbb{Q}$, such curves do not exist by the combined work of Bump–Friedberg–Hoffstein [3], Murty–Murty [11], and Waldspurger [14]. In fact, it is conjectured that half of all quadratic twists of an elliptic curve over $\mathbb{Q}$ have rank 0. Moreover, if $E/\mathbb{Q}$ has no cyclic 4-isogeny, then there exists a quadratic extension $F/\mathbb{Q}$ such that the 2-Selmer group of E over F is the same as over $\mathbb{Q}$ [13, Theorem 1], [10, Theorem 1.5], [9, Theorems 1.1 and 1.3].

As we shall show, however, if we allow only slightly bigger extensions of $\mathbb{Q}$ than quadratic, then there are lots of elliptic curves over $\mathbb{Q}$ whose Selmer groups grow in all such extensions. Below, $S^p(E/F)$ will denote the p-Selmer group of E over a number field F.

Theorem 1.1. *Let E/K be a semistable elliptic curve over a number field with rank r and with n_- primes of non-split multiplicative reduction, satisfying $r > n_-$.*

1. *Let p be an odd prime such that $Ш(E/K)[p^\infty]$ is finite. Then we have that for every Galois extension F/K with Galois group D_{2p}, the dihedral group of order p, either the p-primary part of the Tate-Shafarevich group changes at some step in F/K, or $E(F) \supsetneq E(K)$.*
2. *If p is an odd prime such that $Ш(E/K)[p] = 0$, then for every D_{2p}-extension F/K, either $\#Ш(E/F)[p^\infty] > \#Ш(E/K)[p^\infty]$, or $E(F) \supsetneq E(K)$.*
3. *If p is an odd prime such that $Ш(E/K)[p] = 0$ and $E(K)[p] = 0$, then for every D_{2p}-extension F/K, we have $\#S^p(E/F) > \#S^p(E/K)$.*

Theorem 1.2. *Let E/K be a semistable elliptic curve over a number field with rank r and with n_- primes v of non-split multiplicative reduction for* *which* $\mathrm{ord}_v(\Delta(E))$ *is even, satisfying* $r > n_-$. *Assume that* $\text{Ш}(E/K)[2^\infty]$ *is finite.*

(1) *For every bi-quadratic extension* F/K*, either the* 2*-primary part of the Tate-Shafarevich group changes at some step in* F/K*, or* $E(F) \supsetneq E(K)$.

(2) *If* $\text{Ш}(E/K)[2] = 0$*, then for every bi-quadratic extension* F/K*, either* $\#\text{Ш}(E/F)[2^\infty] > \#\text{Ш}(E/K)[2^\infty]$*, or* $E(F) \supsetneq E(K)$.

(3) *If* $\text{Ш}(E/K)[2] = 0$ *and* $E(K)[2] = 0$*, then for every bi-quadratic extension* F/K*, we have* $\#S^2(E/F) > \#S^2(E/K)$.

Theorem 1.3. *Let* E/K *be a semistable elliptic curve over a number field with* $\mathrm{rk}(E/K) > 0$.

(1) *Let* p *be an odd prime such that* $\text{Ш}(E/K)[p^\infty]$ *is finite. Then we have that for every Galois extensions* F/K *with Galois group* $C_p \times C_p$ *or* $C_p \rtimes C_q$*,* C_q *of prime order, acting faithfully on* C_p*, either the* p*-primary part of the Tate-Shafarevich group changes at some step in* F/K*, or* $E(F) \supsetneq E(K)$.

(2) *If* p *is an odd prime such that* $\text{Ш}(E/K)[p] = 0$*, then for all Galois extensions* F/K *with Galois group* $C_p \times C_p$ *or* $C_p \rtimes C_q$*, either* $\#\text{Ш}(E/F)[p^\infty] > \#\text{Ш}(E/K)[p^\infty]$*, or* $E(F) \supsetneq E(K)$.

(3) *If* p *is an odd prime such that* $\text{Ш}(E/K)[p] = 0$ *and* $E(K)[p] = 0$*, then for all Galois extensions* F/K *with Galois group* $C_p \times C_p$ *or* $C_p \rtimes C_q$*, we have* $\#S^p(E/F) > \#S^p(E/K)$.

Example 1.4. The first few curves over $\mathbb{Q}$ in Cremona's database that satisfy the hypotheses (2) of all three theorems for all primes p are 91b1, 91b2, 91b3, 123a1, 123a2, 141a1, 142a1, 155a1, all of rank 1 and with no primes of non-split multiplicative reduction, and with trivial Tate-Shafarevich groups [8]. Out of these, 91b3, 123a2, 141a1, 142a1 have trivial torsion subgroup over $\mathbb{Q}$ and thus satisfy the stronger hypotheses (3) of all three theorems for all primes p.

Also, the huge majority of rank 2 curves over $\mathbb{Q}$ are expected to have trivial Tate-Shafarevich groups [4]. For example the curve with Cremona label 389a1 almost certainly satisfies the hypotheses (3) of all three theorems for all primes p. Unfortunately, we do not even know that the Tate-Shafarevich group is finite for a single rank 2 elliptic curve. In principle, triviality of the p-part for any fixed prime p can be checked algorithmically (see [12] and the references therein).

Example 1.5. The following example illustrates that the above results are not a parity phenomenon. Let E be the curve with Cremona label 65a1. It has rank 1 over $\mathbb{Q}$ and square-free discriminant, so that the basic conditions of Theorem 1.2 are satisfied. Moreover, $\text{Ш}(E/\mathbb{Q})$ is trivial, so the conclusion of Theorem 1.2 (2) holds for this curve. Let F be the bi-quadratic field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Then we have $E(\mathbb{Q}) = E(F)$. However, $\text{Ш}(E/F)[2] \cong C_2 \times C_2$, as predicted by Theorem 1.2. This cannot be detected by root numbers.

We will collect the necessary ingredients of the proof in great generality, with no assumption on the Galois group of the extension F/K, although we will simplify the exposition by assuming early on that E is semistable.

Then we will perform the necessary calculations in the case of dihedral and bi-quadratic extensions, thereby proving Theorems 1.1 and 1.2.

In the last section, we will discuss generalisations to other Galois groups, such as $C_p \times C_p$ and $C_p \rtimes C_q$, where C_q is of prime order, acting faithfully on C_p. We will also explain why our approach cannot be pushed any further than that. This will rely on a certain representation theoretic classification [2, Corollary 9.2].

Acknowledgements. I would like to thank Vladimir Dokchitser for several very helpful remarks.

2. Tamagawa numbers and regulators

Definition 2.1. Let G be a finite group. A formal $\mathbb{Z}$-linear combination of representatives of conjugacy classes of subgroups $\Theta = \sum_H n_H H$ is called a *Brauer relation* if the virtual permutation representation $\bigoplus \mathbb{C}[G/H]^{\oplus n_H}$ is zero.

Let E/K be an elliptic curve over a number field, F/K a Galois extension with Galois group G, and $\Theta = \sum_H n_H H$ a Brauer relation. There is a corresponding relation between L-functions of E over the intermediate fields:

$$\prod_H L(E/F^H, s)^{n_H} = 1.$$

If E has finite Tate-Shafarevich groups over all intermediate extensions of F/K, then a combination of various compatibility results on the Birch and Swinnerton-Dyer conjecture (see [7, Theorem 2.3]) yields a relation between invariants of E over the intermediate fields:

$$\prod_H \left(\frac{C(E/F^H) \# \text{Ш}(E/F^H) \operatorname{Reg}(E/F^H)}{|E(F^H)_{\text{tors}}|^2} \right)^{n_H} = 1. \tag{2.2}$$

Moreover, if only the p-primary parts of the Tate-Shafarevich groups are assumed to be finite for some prime p, then the p-part of equation (2.2) holds. Note that since each of the regulators is some real number, in general transcendental, it does not make any sense to speak of its p-part. However, since the quotient $\prod_H \operatorname{Reg}(E/F^H)^{n_H}$ is a rational number (this is an immediate consequence of [5, Theorem 2.17]), it does make sense to speak of the p-parts of the regulator quotient and of the remaining terms.

Here, C denotes the product of suitably normalised Tamagawa numbers over the finite places. We do not need to say anything more about the normalisations, since we will only work with semistable elliptic curves (c.f. Assumption 2.4 below), and for those the normalisations cancel in Brauer relations, and we can replace C by products of the usual Tamagawa numbers. See also [1, Remark 2.3].

Recall that the regulator of an elliptic curve is the determinant of the Néron-Tate height pairing evaluated on any basis of the free part of the Mordell-Weil group. The precise normalisation of the pairing that enters the Birch and Swinnerton-Dyer conjecture will be crucial for us. If M/K is a finite extension of fields, and if $\langle \cdot, \cdot \rangle_K$, respectively $\langle \cdot, \cdot \rangle_M$ denotes the Néron-Tate height pairing on $E(K)$, respectively on $E(M)$, then for any $P, Q \in E(K)$, $\langle P, Q \rangle_M = [M : K] \langle P, Q \rangle_K$. In particular, if E/K does not acquire any new points of infinite order over F, then the regulator quotient in (2.2) does not vanish in general, but rather

$$\prod_H \operatorname{Reg}(E/F^H)^{n_H} = \prod_H \frac{1}{|H|^{n_H \operatorname{rk} E(K)}}. \tag{2.3}$$

Fix a prime p, let F/K be one of the extensions described in Theorems 1.1, 1.2, 1.3. If the p-part of the Tate-Shafarevich group over one of the intermediate fields is infinite or if E/K acquires new points of infinite order over F, or if $\#E(F)[p^\infty] > \#E(K)[p^\infty]$, then the conclusions of all three theorems hold. Indeed, this is obvious for conclusions (1) and (2) of all three theorems. For (3), let us note that if $\operatorname{rk} E(F) > \operatorname{rk} E(K)$, then certainly $\#S^p(E/F) > \#S^p(E/K)$. If on the other hand a point of infinite order on $E(K)$ becomes p-divisible over F, then, since F/K is Galois, Kummer theory implies that $E(F)$ must have non-trivial p-torsion. So the assumption that $E(K)[p] = 0$ again forces $\#S^p(E/F) > \#S^p(E/K)$.

For the purpose of proving all three theorems, we may therefore once and for all make the following

Assumption 2.4. Assume that $Ш(E/F)[p^\infty]$ is finite (and consequently, by the inflation-restriction exact sequence, so are the p-primary parts of the Tate-Shafarevich groups over all subfields), and that therefore the p-part of equation (2.2) is true. Moreover, assume that $E(F)/\operatorname{tors} = E(K)/\operatorname{tors}$, so that equation (2.3) holds, and that $E(F)[p^\infty] = E(K)[p^\infty]$. Finally, assume that E is semistable. In particular, C in equation (2.2) can be replaced by the usual Tamagawa numbers.

Equation (2.2) now becomes

$$\prod_H \#Ш(E/F^H)^{n_H} c(E/F^H)^{n_H} =_{p'} \prod |H|^{n_H \operatorname{rk} E(K)}, \tag{2.5}$$

where $c(E/F^H)$ is the product of Tamagawa numbers at the finite places of F^H. Here, $=_{p'}$ denotes equality of p-parts.

3. Dihedral and bi-quadratic extensions

Suppose that $G = D_{2p}$, where p is an odd prime. There is a Brauer relation in G of the form $\Theta = 1 - 2C_2 - C_p + 2G$. For this relation, we have

$$\prod |H|^{n_H} = \frac{(2p)^2}{4p} = p,$$

so that the right hand side of equation (2.5) is $p^{\operatorname{rk} E(K)}$. If v is a place of K, write $c_v(E/K)$ for the Tamagawa number at v, and $c_v(E/F^H)$ for the product of Tamagawa numbers at places of F^H above v. Write $c_v(E/\Theta)$ for the quotient $\frac{c_v(E/K)^2 c_v(E/F)}{c_v(E/F^{C_2})^2 c_v(E/F^{C_p})}$. Similarly, write $\#Ш(E/\Theta)[p^\infty]$ for the p-primary part of the corresponding quotient of sizes of Tate-Shafarevich groups. Finally, let M denote the intermediate quadratic extension $M = F^{C_p}$. The following table gives the possible values of the p-part of $c_v(E/\Theta)$, depending on the reduction type of E at v (horizontal axis) and on the splitting behaviour of v in F/K (vertical axis):

redn. type of E	split mult.	non-split mult.	non-split mult. over K,
splitting of v	over K	over F	split mult. over M
splits into more than one prime	1	1	1
inert in M/K, ramified in F/M	$1/p$	—	p
totally ramified in F/K	$1/p$	1	—

It follows immediately from this table and from equation (2.5) that, under Assumption 2.4, if the rank of E/K is greater than the number of primes of non-split multiplicative reduction, then $\#Ш(E/\Theta)[p^\infty]$ has positive p-adic valuation, and thus at least one of $\#Ш(E/K)[p^\infty]$, $\#Ш(E/F)[p^\infty]$ is strictly larger than at least one of $\#Ш(E/M)[p^\infty]$, $\#Ш(E/F^{C_2})[p^\infty]$. This concludes the proof of Theorem 1.1.

Now, let $G = C_2 \times C_2$, and denote the three distinct subgroups of order 2 by C_2^a, C_2^b, C_2^c. The space of Brauer relations in G is generated by the relation $\Theta = 1 - C_2^a - C_2^b - C_2^c + 2G$, for which we have

$$\prod |H|^{n_H} = \frac{16}{8} = 2.$$

Again writing $c_v(E/\Theta)$ for the corresponding quotient of Tamagawa numbers of E at places above v over the corresponding intermediate fields of F/K, the following table gives the possible values of $c_v(E/\Theta)$

redn. type of E	split mult.	non-split mult.	non-split mult. over K,
splitting of v	over K	over F	split mult. over some F^{C_2}
splits in some F^{C_2}	1	1	1
inert in some F^{C_2}/K, ramified in F/F^{C_2}	$1/2$	—	2: $\mathrm{ord}_v(\Delta(E))$ is even 1/2: otherwise
totally ramified in F/K	$1/2$	1: $\mathrm{ord}_v\,\Delta(E)$ even 1/4: otherwise	—

As above, this table together with equation (2.5) proves Theorem 1.2.

4. Generalisation to other Galois groups

If G is a subgroup of a group $\tilde{G}$, then by transitivity of induction, a Brauer relation Θ in G automatically gives a Brauer relation $\mathrm{Ind}_{\tilde{G}/G}\,\Theta$ in $\tilde{G}$. Also, if G is a quotient of a group Γ, $G = \Gamma/N$, then a Brauer relation $\Theta = \sum_H n_H H$ in G gives rise to a Brauer relation $\mathrm{Inf}_{\Gamma/N}\,\Theta = \sum_H n_H NH$ in Γ.

In general, in order to prove by the same technique as above that the p-Selmer group of some elliptic curve grows in all Galois extensions with Galois group G, we need to have a Brauer relation $\Theta = \sum_H n_H H$ in G such that $\mathrm{ord}_p(\prod |H|^{n_H}) \neq 0$. This quantity is clearly invariant under inductions and lifts of Brauer relations.

Proposition 4.1 ([2], Corollary 9.2)**.** *Let p be a prime number. A finite group $\tilde{G}$ has a Brauer relation $\Theta = \sum_H n_H H$ with $\mathrm{ord}_p(\mathcal{C}_\Theta(\mathbf{1})) \neq 0$ if and only if $\tilde{G}$ has a subquotient G isomorphic either to $C_p \times C_p$ or to $C_p \rtimes C_q$ with C_q cyclic of prime order acting faithfully on C_p. Moreover, in the* *former case Θ can be taken to be induced and/or lifted from the relation $1-\sum_{U\leq_p G} U + pG$; while in the latter case Θ can be taken to be induced and/or lifted from the relation $1-qC_q-C_p+qG$.*

Clearly, if the p-Selmer group of E/K grows in all Galois extensions with Galois group G, then it also grows in all extensions whose Galois group has a quotient isomorphic to G. The same is not true if "quotient" is replaced by "subgroup". But if $\tilde{G}$ contains G and if some conditions on the rank of E and the number of primes of given reduction type force p-Selmer groups of E to grow in G-extensions of number fields, as in the previous section, then stronger conditions on the rank and the number of primes will yield the same conclusions for $\tilde{G}$-extensions F/K, by applying the result on G-extensions to F/F^G. Thus, we may restrict attention to the groups $C_p\times C_p$ and $C_p\rtimes C_q$ as in the proposition.

When $G=C_p\times C_p$ and $\Theta = 1-\sum_{U\leq_p G} U + pG$, we have

$$\prod |H|^{n_H} = \frac{(p)^{2p}}{p^{p+1}} = p^{p-1}.$$

When $G=C_p\rtimes C_q$ and $\Theta=1-qC_q-C_p+qG$, we have

$$\prod |H|^{n_H} = \frac{(pq)^q}{pq^q} = p^{q-1}.$$

Having already dealt with such groups of even order, we may now restrict our attention to groups of odd order, so that only the primes of K at which E has split multiplicative reduction contribute to the corresponding Tamagawa number quotients.

Here are the possible values of $c_v(E/\Theta)$ when E/K has split multiplicative reduction at v, first for $G=C_p\times C_p$ and $\Theta=1-\sum_{U\leq_p G} U + pG$, and then for $G=C_p\rtimes C_q$ and $\Theta = 1-qC_q-C_p+qG$, where p and q are odd primes:

v splits	v is inert in some F^{C_p}/K and ramified in F/F^{C_p}	v is totally ramified
1	p^{1-p}	p^{1-p}

,

v splits	v is inert in F^{C_p}/K and ramified in F/F^{C_p}	v is totally ramified
1	p^{1-q}	p^{1-q}

.

These tables together with equation (2.5) finish the proof of Theorem 1.3.

References

[1] A. Bartel, Large Selmer groups over number fields, Math. Proc. Cambridge Philos. Soc. **148** (2010), 73–86.

[2] A. Bartel, T. Dokchitser, Brauer relations in finite groups, arXiv:1103.2047v2 [math.RT].

[3] D. Bump, S. Friedberg, J. Hoffstein, Nonvanishing theorems for L-functions of modular forms and their derivatives, Invent. Math. **102** (1990), 543–618.

[4] C. Delaunay, Heuristics on class groups and on Tate–Shafarevich groups: the magic of the Cohen–Lenstra heuristics, in Ranks of Elliptic Curves and Random Matrix Theory, London Math. Soc. Lecture Note Series 341, Cambridge Univ. Press, Cambridge, 2007, 323–340.

[5] T. Dokchitser, V. Dokchitser, Regulator constants and the parity conjecture, Invent. Math. **178** no. 1 (2009), 23–71.

[6] T. Dokchitser, V. Dokchitser, Elliptic curves with all quadratic twists of positive rank, Acta Arith. **137** (2009), 193–197.

[7] T. Dokchitser, V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, Annals of Math. **172** no. 1 (2010), 567–596.

[8] G. Grigorov, A. Jorza, S. Patrikis, C. Patrascu, W. Stein, Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, Math. Comp. **78** (2009), 2397–2425.

[9] Z. Klagsbrun, Selmer ranks of quadratic twists of elliptic curves with partial two-torsion, preprint, arXiv:1201.5408v1 [math.NT].

[10] B. Mazur, K. Rubin, Ranks of twists of elliptic curves and Hilbert's tenth problem, Invent. Math. **181** (2010) 541–575.

[11] M. R. Murty, V. K. Murty, Mean values of derivatives of modular L-series, Annals of Math. **133** (1991), 447–475.

[12] M. Stoll, E. F. Schaefer, How to do a p-descent on an elliptic curve, Trans. Amer. Math. Soc. **356** (2004), 1209–1231.

[13] P. Swinnerton-Dyer, The effect of twisting on the 2-Selmer group, Math. Proc. Cambridge Philos. Soc. **145** no. 3 (2008), 513–526.

[14] J.-L. Waldspurger, Correspondances de Shimura et quaternions, Forum Math. **3** (1991), 219–307.

Department of Mathematics, POSTECH, Pohang, Gyungbuk 790-784, Republic of Korea

E-mail address: bartel@postech.ac.kr